The University of Chicago

A FUNDAMENTAL SYSTEM OF INVARIANTS OF A MODULAR GROUP OF TRANSFORMATIONS

A DISSERTATION

SUBMITTED TO THE FACULTY OF THE OGDEN GRADUATE SCHOOL OF SCIENCE
IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY
DEPARTMENT OF MATHEMATICS

BY

JOHN SIDNEY TURNER

Private Edition, Distributed By
The University of Chicago Libraries
Chicago, Illinois

Reprinted from
TRANSACTIONS AMERICAN MATHEMATICAL SOCIETY
Vol. XXIV, No. 2, September, 1922

The University of Chicago

A FUNDAMENTAL SYSTEM OF INVARIANTS OF A MODULAR GROUP OF TRANSFORMATIONS

A DISSERTATION

SUBMITTED TO THE FACULTY OF THE OGDEN GRADUATE SCHOOL OF SCIENCE
IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY
DEPARTMENT OF MATHEMATICS

BY

JOHN SIDNEY TURNER

Private Edition, Distributed By
The University of Chicago Libraries
Chicago, Illinois

Reprinted from
TRANSACTIONS AMERICAN MATHEMATICAL SOCIETY
Vol. XXIV, No. 2, September, 1922

R. UNIV.
BIBLIOTHEEK
LEIDEN

A FUNDAMENTAL SYSTEM OF INVARIANTS OF A MODULAR GROUP OF TRANSFORMATIONS*

BY

JOHN SIDNEY TURNER

1. **Introduction.** Let G be any given group of g homogeneous linear transformations on the indeterminates $x_1, \cdots, x_n$, with integral coefficients taken modulo m. Hurwitz† raised the question of the existence of a finite fundamental system of invariants of G in the case where m is a prime p, and obtained an affirmative answer when g is prime to p. Dickson‡ subsequently obtained an affirmative answer for any g.

The general case presents great difficulty, owing to the fact that resolution into irreducible factors with respect to a composite modulus is not, in general, unique. The present investigation is confined to the case in which there are two indeterminates x, y, and m is the square of a prime p. The given group will be denoted by H, the notation G being retained when $m = p$. It is proved that the $p^2 + 1$ invariants

$$L^p, Q^p, pL^\alpha Q^\beta \qquad (\alpha, \beta = 0, 1, \cdots, p-1; \alpha, \beta \text{ not both zero}),$$

where

$$L = yx^p - xy^p, \qquad Q = (x^{p^2-1} - y^{p^2-1})/(x^{p-1} - y^{p-1}),$$

form a fundamental system of (independent) invariants of the group H.

2. Consider the group H of all linear homogeneous transformations modulo p^2:

$$(1) \qquad x' \equiv ax + by, \qquad y' \equiv cx + dy, \qquad ad - bc \equiv 1 \pmod{p^2},$$

where a, b, c, d are integers. To each transformation of H corresponds a unique transformation of the group G:

$$(2) \qquad x' \equiv a_1 x + b_1 y, \qquad y' \equiv c_1 x + d_1 y, \qquad a_1 d_1 - b_1 c_1 \equiv 1 \pmod{p},$$

where a_1, b_1, c_1, d_1 are integers. In fact, we have only to choose

$$a_1 \equiv a, \qquad \cdots, \qquad d_1 \equiv d \pmod{p}.$$

Conversely, to each transformation (2) corresponds one or more transformations (1). For, we can choose $a \equiv a_1, \cdots, d \equiv d_1 \pmod{p}$ so that

* Presented to the Society, April 15, 1922.

† Archiv der Mathematik und Physik (3), vol. 5 (1903), p. 25.

‡ *The Madison Colloquium*, Lect. III.

$ad - bc \equiv 1 \pmod{p^2}$. For example, if $a_1 \not\equiv 0 \pmod{p}$ we may take $a \equiv a_1$, $b \equiv b_1$, $c \equiv c_1 \pmod{p}$, and determine d by $ad - bc \equiv 1 \pmod{p^2}$; evidently $d \equiv d_1 \pmod{p}$.

Hence if we reduce all the transformations of H modulo p, we obtain all the transformations of G.

3. **Definition.** A rational and integral invariant of H is a polynomial $I(x, y)$ in x and y with integral coefficients, which remains unchanged modulo p^2 under every transformation (1). That is,

$$I(x', y') \equiv I(ax + by, cx + dy) \equiv I(x, y) \pmod{p^2} \tag{3}$$

for all integers $a, \cdots, d$ such that $ad - bc \equiv 1 \pmod{p^2}$.

Evidently any rational and integral invariant is a sum of homogeneous invariants; hence we restrict the investigation to the latter.

4. THEOREM I. *Let $I(x, y)$ be a rational and integral invariant of H, and let $I_1(x, y)$ be the polynomial obtained from $I(x, y)$ by replacing each coefficient by its positive or zero residue modulo p. Then $I_1(x, y)$ will be a rational and integral invariant of G.*

We have (3) for all transformations of H. Now

$$I(x, y) \equiv I_1(x, y) \pmod{p}$$

and

$$I(ax + by, cx + dy) \equiv I_1(ax + by, cx + dy) \equiv I_1(a_1 x + b_1 y, c_1 x + d_1 y) \pmod{p},$$

hence

$$I_1(x', y') \equiv I_1(a_1 x + b_1 y, c_1 x + d_1 y) \equiv I_1(x, y) \pmod{p}, \tag{4}$$

and by § 2 this is true for all transformations of G.

5. Now (*Madison Colloquium*, pp. 34–38),

$$I_1(x, y) \equiv k T_1^{\alpha_1} T_2^{\alpha_2} \cdots T_i^{\alpha_i} \cdots T_r^{\alpha_r} * \pmod{p},$$

where k is an integer,

$$T_1 = L, \qquad T_2 = Q, \qquad T_i = R_i(L^{\frac{1}{2}p(p-1)}, \dagger\ Q^{\frac{1}{2}(p+1)}) \qquad (i = 3, 4, \cdots, r)$$

R_i being a polynomial in its two arguments, with integral coefficients; moreover the T_i $(i = 1, 2, \cdots, r)$ contain no multiple factors, and are relatively prime modulo p. Hence

$$I(x, y) \equiv k T_1^{\alpha_1} T_2^{\alpha_2} \cdots T_i^{\alpha_i} \cdots T_r^{\alpha_r} + pF(x, y) \pmod{p^2}, \tag{5}$$

where $F(x, y)$ denotes a polynomial in x, y with integral coefficients.

* In the discussion which follows, if any α_i is zero the corresponding T_i is to be suppressed.

† If $p = 2$, we omit the divisor 2 in the exponents.

6. Discussion of equation (5). Apply to $I(x, y)$ the transformation

$$x' \equiv x + py, \qquad y' \equiv y \pmod{p^2}, \tag{6}$$

expand by Taylor's Theorem, and denote the partial derivative of T_i with respect to x by T'_i. Then

$$I(x + py, y) \equiv I(x, y) + pykT_1^{\alpha_1 - 1} \cdots T_i^{\alpha_i - 1} \times \cdots T_r^{\alpha_r - 1} \sum_{i=1}^{r} \alpha_i T_1 \cdots T_{i-1} T'_i T_{i+1} \cdots T_r \pmod{p^2}. \tag{7}$$

Since (6) is a transformation of H,

$$I(x + py, y) \equiv I(x, y) \pmod{p^2}.$$

Hence either $k \equiv 0 \pmod{p}$, in which case the right member of (5) reduces to its second term, or

$$\sum_{i=1}^{r} \alpha_i T_1 \cdots T_{i-1} T'_i T_{i+1} \cdots T_r \equiv 0 \pmod{p}. \tag{8}$$

Let $(g_i, 1)$ be a point at which $T_i(x, y)$ vanishes. Then, for $j \neq i$, $T_j(x, y)$ cannot vanish at $(g_i, 1)$; for, in that event, $T_j(x, y)$ would be a factor of $T_i(x, y)$ modulo p,* contrary to § 5. Therefore from (8) we have

$$\alpha_i T'_i(g_i, 1) \equiv 0 \pmod{p}. \tag{9}$$

Hence either $\alpha_i \equiv 0$, or $T'_i(g_i, 1) \equiv 0 \pmod{p}$. In the latter case, by a known theorem on Galois imaginaries, $T_i(x, 1)$ and $T'_i(x, 1)$ have a common factor with integral coefficients modulo p. But (§ 5) $T_i(x, 1)$ contains no multiple factor modulo p. Therefore† $T'_i(x, 1) \equiv 0 \pmod{p}$, whence

$$T'_i(x, y) \equiv 0 \pmod{p}. \tag{10}$$

Hence we have

THEOREM II. *In equation* (5), *for each* $i = 1, \cdots, r$, *either* α_i *is a multiple of* p, *or* $T'_i(x, y) \equiv 0 \pmod{p}$.

COROLLARY 1. $\alpha_1 \equiv 0 \pmod{p}$.

For $T_1 = yx^p - xy^p$; hence $T'_1 = pyx^{p-1} - y^p \not\equiv 0 \pmod{p}$.

COROLLARY 2. $\alpha_2 \equiv 0 \pmod{p}$.

For

$$T_2 = x^{p(p-1)} + x^{(p-1)^2} y^{p-1} + \cdots + x^{p-1} y^{(p-1)^2} + y^{p(p-1)},$$

hence $T'_2 \not\equiv 0 \pmod{p}$.

COROLLARY 3. *If* $\alpha_i = p\beta_i$ *for* $i > 2$,

$$T_i^{\alpha_i} \equiv S_i(L^p, Q^p) \pmod{p}, \tag{11}$$

where S_i *is a polynomial in its arguments, with integral coefficients.*

* *The Madison Colloquium*, p. 38.

† Dickson, *Lecture Notes on Double Modulus and Galois Imaginaries*, § 5.

For if we expand

$$T_i^{\alpha_i} = [R_i(L^{\frac{1}{2}p(p-1)}, Q^{\frac{1}{2}(p+1)})]^{p\beta_i},$$

we observe that in each term the exponent of L is a multiple of p and that either the exponent of Q or the coefficient of the term is a multiple of p.

7. **Discussion of** $T_i'(x, y) \equiv 0 \pmod{p}$. Write

$$T_i(x, y) = \sum_{r=0}^{n} A_r l^{n-r} q^r, \tag{12}$$

where $l = L^{\frac{1}{2}p(p-1)}$,* $q = Q^{\frac{1}{2}(p+1)}$, and the coefficients A_r are integers; then

$$T_i'(x, y) = \sum_{r=0}^{n-1} A_r(n-r) l^{n-r-1} l' q^r + \sum_{r=1}^{n} A_r r l^{n-r} q^{r-1} q' \equiv 0 \pmod{p},$$

where l', q' denote the partial derivatives of l, q with respect to x. Evidently $l' \equiv 0$, $q' \not\equiv 0 \pmod{p}$; therefore

$$\sum_{r=1}^{n} r A_r l^{n-r} q^{r-1} \equiv 0 \pmod{p}. \tag{13}$$

Each term of (13) is the product of the preceding by cq/l, c a constant; the degree in x of q/l is $\frac{1}{2}(p^2 - p)$,† hence the degrees in x of the successive terms increase by $\frac{1}{2}(p^2 - p)$. Equating coefficients of x, we find in succession

$$nA_n \equiv 0, \quad \cdots, \quad rA_r \equiv 0, \quad \cdots, \quad A_1 \equiv 0 \pmod{p}.$$

Hence in each term of $\sum_{r=1}^{n} A_r l^{n-r} q^r$, either the coefficient A_r or the exponent of q is a multiple of p, and we have

THEOREM III. *If* $T_i'(x, y) \equiv 0 \pmod{p}$, *then*

$$T_i(x, y) \equiv S_i(L^p, Q^p) \pmod{p}, \tag{14}$$

where S_i *denotes a rational and integral function of its arguments, with integral coefficients.*

COROLLARY. $[T_i(x, y)]^{\alpha_i}$ *is a polynomial in* L^p, Q^p, *with integral coefficients, modulo* p.

8. THEOREM IV. L^p *is invariant under the group* H.

Write $L(x', y') = e$, $L(x, y) = f$, where x', y' are derived from x, y by any transformation (2) of the group G; then‡ $e - f \equiv 0 \pmod{p}$. Hence $e - f \equiv 0 \pmod{p}$ for every transformation (1) of H. For if, as in § 2, we choose $a_1 \equiv a, \cdots, d_1 \equiv d$ modulo p, we have

$$L(ax + by, cx + dy) \equiv L(a_1 x + b_1 y, c_1 x + d_1 y) \equiv L(x, y) \pmod{p}.$$

* If $p = 2$, we omit the divisor 2 in the exponents.

† If $p = 2$, the degree is 2.

‡ *The Madison Colloquium*, p. 35.

Also

$$e^p - f^p = (e - f + f)^p - f^p$$
$$= (e - f)[(e - f)^{p-1} + \cdots + \tfrac{1}{2}p(p-1)(e-f)f^{p-2} + pf^{p-1}],$$

and each factor on the right is identically congruent to zero modulo p; hence $e^p - f^p \equiv 0 \pmod{p^2}$; that is

$$[L(ax + by, cx + dy)]^p \equiv [L(x, y)]^p \pmod{p^2}$$

for every transformation of H.

COROLLARY 1. *In the same way, it can be proved that Q^p is invariant under the group H.*

COROLLARY 2. *$pL^\alpha Q^\beta$ is invariant under the group H.*

9. THEOREM V. *Any rational and integral invariant of the group H is a rational and integral function, with integral coefficients, of the $p^2 + 1$ invariants L^p, Q^p, $pL^\alpha Q^\beta$ ($\alpha, \beta = 0, 1, \cdots, p-1$; α, β not both zero). Conversely, any such function is an invariant of H.*

In (5), the term $kT_1^{\alpha_1} T_2^{\alpha_2} \cdots T_r^{\alpha_r}$ is an invariant of H. For if any $\alpha_i \equiv 0 \pmod{p}$, then by Theorems II and IV with their corollaries, $T_i^{\alpha_i}$ is an invariant; $T_1 = L$, $T_2 = Q$, $\alpha_1 \equiv \alpha_2 \equiv 0 \pmod{p}$. While if $\alpha_j \not\equiv 0 \pmod{p}$, $T_j' \equiv 0$, and by Theorems III and IV with their corollaries $T_j^{\alpha_j}$ is an invariant.

Hence the second term $pF(x, y)$ of (5) is an invariant of H, and it follows from § 2 that $F(x, y)$ is an invariant of G. Therefore $pF(x, y)$ is the product of p by a polynomial in L and Q. It follows that if $I(x, y)$ is any rational and integral invariant of H,

$$I(x, y) \equiv S(L^p, Q^p, pL^\alpha Q^\beta) \pmod{p^2}, \tag{15}$$

where $pL^\alpha Q^\beta$ denotes the set pL, pQ, pL^2, pLQ, $\cdots$, $pL^{p-1}Q^{p-1}$, and S denotes a rational and integral function of its arguments, with integral coefficients.

Conversely, any rational and integral function of L^p, Q^p, $pL^\alpha Q^\beta$, with integral coefficients, is a sum of invariants, and is therefore itself an invariant. Hence these $p^2 + 1$ invariants form a fundamental system.

10. THEOREM VI. *The invariants of the fundamental system are independent.*

In view of the coefficients p, neither L^p nor Q^p can be expressed as a polynomial in the remaining invariants, with integral coefficients. Assume that $pL^{\alpha_1} Q^{\beta_1}$, $\alpha_1 \leqq p - 1$, $\beta_1 \leqq p - 1$, can be so expressed. Then

$$pL^{\alpha_1} Q^{\beta_1} \equiv P(L^p, Q^p, pL^\alpha Q^\beta) \pmod{p^2} \tag{16}$$

identically in x, y. We may suppose that P contains no group of terms which vanishes identically modulo p^2. Let $mL^{\alpha_2} Q^{\beta_2}$ be any term of P; then $pL^{\alpha_1} Q^{\beta_1}$ and $mL^{\alpha_2} Q^{\beta_2}$ must be of the same total degree in x, y, and also of the same

degree in x alone. Therefore

$$\alpha_1(p+1)+\beta_1 p(p-1)=\alpha_2(p+1)+\beta_2 p(p-1),$$
$$\alpha_1 p+\beta_1 p(p-1)=\alpha_2 p+\beta_2 p(p-1),$$

whence $\alpha_1=\alpha_2$, $\beta_1=\beta_2$. Hence P consists of the single term $pL^{\alpha_1}Q^{\beta_1}$. Evidently $pL^{\alpha_1}Q^{\beta_1}$ is not a product of fundamental invariants, hence the theorem is proved.

11. If we consider the total group

$$(17)\qquad \begin{aligned} x' &\equiv ax+by, \quad y' \equiv cx+dy && (\mathrm{mod}\ p^2),\\ ad-bc &\not\equiv 0 && (\mathrm{mod}\ p), \end{aligned}$$

we find, exactly as in Theorem IV, that Q^p is an absolute invariant, and that L^p, $pL^\alpha Q^\beta$ are relative invariants of indices p, α, respectively.

IOWA STATE COLLEGE,
AMES, IOWA.

BIOGRAPHY

John Sidney Turner was born at Liverpool, England, on Sept. 4th, 1884. He was educated at Warbreck College, Aintree, and at Liverpool College. In 1903 he won an Open Mathematical Scholarship at Selwyn College, Cambridge, and graduated B.A. (11th Senior Optime) in 1906. He was Lecturer at Bishop's College, Lennoxville, P. Q., Can., during 1906–8, and Lecturer and Professor at King's College, Windsor, N. S., Can., during 1909–11.

He studied at Harvard Univ. in 1911–12. He was Instructor at the Univ. of Arkansas during 1912–15, and at the Univ. of Minnesota in 1915–16. He was awarded a Fellowship and studied at the Univ. of Chicago in 1916–17. During the war he served in the Canadian Army and at the British Admiralty. He was Professor at Alabama Polytechnic Institute in 1920–21, and was appointed Assistant Professor at Iowa State College in 1921. At Chicago he studied under Professors Bliss, Bolza, Dickson, Laves, Lefschetz, Lunn, Moore, Moulton, and Wilczynski. To all of these, and especially to Professor Dickson under whom this thesis was written, he tenders his thanks for their excellent instruction and unfailing kindliness.